UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

GLOBALIZATION PARTNERS LLC Plaintiff, v. DOES 1-4, Defendants.	CIVIL ACTION NO. 24-cv-11144

COMPLAINT

Plaintiff, Globalization Partners LLC ("G-P"), asserts the following claims against Defendants, Does 1-4.

PARTIES

1. Plaintiff G-P is a limited liability company duly organized and existing under the laws of the State of Delaware, with its principal place of business in Boston, Massachusetts.

2. The true name, capacity, and number of Defendants is not known to Plaintiff at this time. Plaintiff believes that information obtained in discovery may lead to the identification of Defendants.

JURISDICTION AND VENUE

3. G-P's first cause of action arises under the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030 *et seq*. This Court has subject-matter jurisdiction over this action pursuant to 18 U.S.C. § 1030(g) and 28 U.S.C. § 1331.

4. This Court has supplemental subject matter jurisdiction over the second cause of action for misappropriation of sensitive and/or confidential information under 28 U.S.C. § 1367

because that claim is so related to G-P's claim under federal law that it forms part of the same case or controversy.

5. Venue in this district is appropriate, pursuant to 28 U.S.C. § 1391, because a substantial part of the events giving rise to this dispute occurred in this district; upon information and belief, Defendants are subject to personal jurisdiction in this district.

FACTS

6. Plaintiff G-P provides employer of record, contractor, and other employment related services to companies wishing to expand their workforce internationally. Through providing these services, G-P obtains and stores information about its customers, employees, contractors, banks, vendors and other third parties with whom it conducts business, including, but not limited to, personally identifiable information and email addresses and other contact information. G-P employs practices and procedures to avoid disclosure and/or maintain the confidentiality of this information, including storing the information on secured and encrypted computers and limiting access to only authorized users. The secured and encrypted computers are located in the Commonwealth of Massachusetts and other locations throughout the United States and internationally.

7. On information and belief, on or about March 8, 2024, Defendants conducted a phishing campaign targeting at least four current or former members of G-P's Treasury and Finance teams. Two of the targets are active employees and the other two targets are former employees with inactive G-P network accounts.

8. On information and belief, one of the current members of G-P's Treasury team ("G-P Treasury Employee No. 1") clicked one or more of a series of links and scanned a QR code with

their mobile device.[1] The QR code contained a URL which led to a fake Microsoft authentication webpage where G-P Treasury Employee No. 1 was prompted to login with their corporate account. As a result (and as was their intention), Defendants were able to obtain G-P Treasury Employee No. 1's credentials, which were used to obtain unauthorized access to their G-P account.

9. On information and belief, the Defendants then used this access to establish a Dropbox account in the name of G-P Treasury Employee No. 1.

10. On information and belief, on or about March 18, 2024, Defendants used the Dropbox account purporting to be G-P Treasury Employee No. 1 to send a link to a Dropbox file to several G-P customers, banks, contractors, and vendors (the "Recipients").

11. On March 18, 2024, G-P became aware of these activities and took immediate steps to freeze the G-P Treasury Employee No. 1's G-P accounts and reset their internal G-P credentials. Even so, several of the Recipients forwarded the faked Dropbox message to G-P Treasury Employee No. 1, asking if the Dropbox email was legitimate.

12. On March 19, 2024, G-P contacted Dropbox through ordinary business channels and also notified a member of the Dropbox Board of Directors to assist in contacting the appropriate leadership at Dropbox. Upon G-P's request, Dropbox froze the fake Dropbox account established by the Defendants.

13. G-P subsequently requested additional information from Dropbox, including the names and email addresses of all who were contacted by the Defendants via the fake Dropbox account.

[1] A QR or "quick response" code is a machine-readable code consisting of an array of black and white squares, typically used for storing uniform resource locators ("URLs") or other information for reading by the camera on a smartphone.

G-P sought this information so that it could ascertain the scope of this incident. G-P has not yet received the additional requested information from Dropbox.

14. On or about March 23, 2024, another current employee in G-P's Sales Department was targeted, which G-P believes was part of Defendants' same campaign. G-P is still investigating this incident.

15. On information and belief, Defendants gained unauthorized access or exceeded authorized access to G-P's computers and obtained sensitive and/or confidential information contained on those computers.

16. The identities and email addresses of certain of the G-P employees and the Recipients that Defendants contacted are not generally known outside of G-P. Defendants' knowledge of these people and their email addresses and Defendants' potential access to other sensitive and/or confidential information contained on G-P's secured and encrypted computers may be attributed to Defendants' improperly obtained knowledge of G-P's operations, personnel, and computer systems.

17. Defendants' access to and use of G-P's sensitive and/or confidential information was unlawful.

COUNT I
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT

18. Plaintiff incorporates by reference and realleges all of the preceding paragraphs as though fully set forth herein.

19. The computer system that Defendants accessed as described above is used in or affecting interstate commerce or communication, and as such constitutes a "protected computer" within the meaning of 18 U.S.C. § 1030(e)(2).

20. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, and by obtaining information from such a protected computer.

21. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4) by knowingly, and with intent to defraud G-P and/or others, accessing a protected computer, without authorization or by exceeding authorized access to such a computer, and by means of such conduct furthered the intended fraud and obtained one or more things of value, including credential information of G-P employees, contact information for G-P customers, banks, and other vendors, and confidential information that G-P Treasury Employee No. 1 used to conduct financial transactions on behalf of G-P.

22. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(B) by intentionally accessing a protected network without authorization, and as a result of such conduct, caused damage.

23. On information and belief, G-P has suffered damage and loss by reason of these violations in an amount to be proved at trial, but, in any event, in an amount over $5,000 aggregated over a one-year period.

24. Defendants' unlawful access to and theft from G-P's networks have also caused G-P irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. G-P's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling G-P to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

COUNT II
MISAPPROPRIATION OF SENSITIVE AND/OR CONFIDENTIAL INFORMATION

25. Plaintiff incorporates by reference and realleges all of the preceding paragraphs as though fully set forth herein.

26. The credential information of G-P employees, contact information for G-P customers, banks, and other vendors, and confidential information that G-P Treasury Employee No. 1 used to conduct financial transactions on behalf of G-P in G-P's possession is sensitive and/or confidential information. Plaintiff has expended significant time and expense to safeguard and preserve its confidentiality and/or prevent its disclosure.

27. Defendants intentionally and wrongfully misappropriated and/or converted for their own use G-P's sensitive and/or confidential information. Defendants' conduct was inconsistent with and interfered with G-P's interests in the sensitive and/or confidential information and its right and/or duty to keep that information from being disclosed.

28. Defendants obtained G-P's sensitive and/or confidential information through improper means and/or are improperly using G-P's sensitive and/or confidential information for Defendants' own benefit.

29. As a direct and proximate result of Defendants' unlawful actions, G-P is in imminent danger of irreparable harm and has been and will continue to suffer substantial damages.

PRAYER FOR RELIEF

WHEREFORE, G-P respectfully requests that the Court grant the following relief:

A. An injunction requiring Defendants to:

a. Cease and desist from any efforts to obtain sensitive and/or confidential information from G-P;

b. Cease and desist transmitting and using sensitive and/or confidential information previously obtained from G-P;

c. Cease and desist from communicating with G-P's personnel or agents, except through counsel;

d. Return all sensitive and/or confidential information that Defendants have obtained from G-P and provide a verified statement under oath that such information has been returned and any remaining copies in Defendants' possession have been destroyed;

B. Damages to be proven at trial;

C. An award of G-P's costs and reasonable attorneys' fees; and

D. Such other and further relief as this Court may deem just and proper.

Respectfully submitted,

GLOBALIZATION PARTNERS LLC
By its attorneys,

Colin J. Zick, Esq. (BBO# 556538)
Daniel T. Carlston, Esq. (BBO# 714078)
FOLEY HOAG LLP
155 Seaport Boulevard
Boston, MA 02210-2600
Phone: (617) 832-1000
czick@foleyhoag.com
dcarlston@foleyhoag.com

Dated: April 29, 2024